

JPL D-48271

Outer Planet Flagship Mission (OPFM) **Long Life Engineering Guidelines**

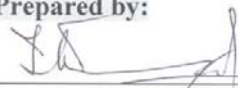
Prepared by

Taher Daud
Ed Shalom
Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, CA 91109

October 18, 2008

Preliminary Version

Prepared by:

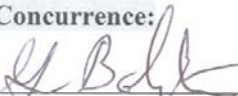

Taher Daud, Sec 345

Date: 10/16/08


Ed Shalom, Sec 3401

Date: 10/15/08

Concurrence:


Gary Bolotin, Manager Sec 3401

Date: 10/16/08

For Public Release

Copyright © 2008 by the California Institute of Technology
Government Sponsorship Acknowledged



Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

Pre-Decisional: for Planning and Discussion Purposes Only

TABLE OF CONTENTS

1.0	SCOPE	1
1.1	Level.....	1
1.2	Effort is Targeted at all Mission Phases.....	1
1.3	Effort is Targeted at both Engineering and Science	1
1.4	Introduction to Long Life Guidelines	2
2.0	REFERENCE DOCUMENTS & EXISTING PRACTICE.....	2
2.1	JPL D-9899, Long Life/High Reliability Design and Test Rules Study Report .2	
2.1.1	Applicability of D-9899	3
2.2	References to Reliability Assurance / Long Life Design Docs.....	3
3.0	SYSTEM CONSIDERATIONS & REQUIREMENTS	4
3.1	Capturing Requirements.....	4
3.2	Flow down Requirements: functional & fault protection	4
3.3	Self-Imposed requirements.....	4
3.4	System-Level Verification and Validation (V&V).....	4
3.4.1	V&V vs. Development Level	4
4.0	ROBUST SYSTEM ARCHITECTURE.....	4
4.1	Inheritance	4
4.2	Hardware vs. Software Trade.....	5
4.3	Partitioning Functionality into Modules	5
4.4	Model Based Engineering (MBE)	5
4.5	Simulation: Part and Board Level.....	5
4.6	Power-On vs. Power Off States.....	6
5.0	FAULT TOLERANCE.....	6
5.1	Highly Featured Fault Protection (FP).....	6
5.2	Providing Resources for FP.....	7
5.3	Beyond Block Redundancy	7
6.0	PARTS AND MATERIALS	7
6.1	Early Part Selection & Generic Parts.....	7
6.2	Approved Parts and Materials List	8
6.3	Long Lead Time Parts ID & Budgeting.....	8
6.4	FPGAs vs. ASICs	8
6.5	SEU Mitigation Techniques for FPGAs	8
6.6	Special Radiation Tests.....	8
7.0	MISSION ASSURANCE & QUALITY ASSURANCE.....	9
7.1	Problem Reporting System.....	9
8.0	VERIFICATION AND VALIDATION (V&V).....	9
8.1	Verification and Validation for a High Radiation Environment	9
8.1.1	V&V of Fault Protection System.....	9
8.2	Engineering Models (EM): Build Early and in Quantity.....	10
9.0	ELECTRONIC PACKAGING.....	10
10.0	Packaging Approach	11
10.1	Printed Wiring Board (PWB) Design Approach.....	11
11.0	THERMAL CONTROL	11
11.1	Tighter Control of Flight Operating Temperatures.....	11
12.0	Transport Analysis: location and orientation of units on S/C.....	12

Pre-Decisional: for Planning and Discussion Purposes Only

13.0	RELIABILITY ANALYSIS PROCESS.....	12
13.1	Debugging the Improved Process.....	12
14.0	RISK MANAGEMENT SYSTEM.....	13
14.1	Risk Analysis.....	14
14.2	Risk Tracking and Control.....	14
15.0	EXTENDING LIFE DURING OPERATIONS.....	14
15.1	Need for Higher Observability.....	15
15.2	Fully Integrated S/C and Ground Fault Protection.....	15
15.3	Complete Parametric Testing of Signatures of Anomalous Behavior.....	15

Appendix A:

Appendix B:

1.0 SCOPE

The scope of this document is to encompass major locations of flight electronics: in the engineering subsystems such as C&DH, Power, and Telecom, and also in the science payload, for the Outer Planet Flagship Mission (OPFM). OPFM includes both the Titan-Saturn System Mission (TSSM) and the Europa-Jupiter System Mission (EJSM).

As such, much of the content of this document addresses both TSSM and EJSM. As appropriate, this document focuses special attention upon the Jupiter Earth Explorer (JEO), which is the NASA component of EJSM, and which is uniquely exposed to high radiation levels.

To a large extent, the long life guidelines are generic; in cases where there is a particular focus upon a specific area, it shall be identified.

1.1 Level

In general, the intent of these guidelines is to address Requirements Level 4 (Subsystem) and below. However, there are cases where it is appropriate to drive requirements at higher levels. In the interest of ensuring that appropriate attention is paid at all levels, this document errs on the side of inclusion.

1.2 Effort is Targeted at all Mission Phases

This document looks at the entire life cycle of a mission in order to identify processes and techniques that could extend the lifetime of S/C avionics. The span of these phases extends from early conceptual design and architecture, through the process of parts selection, design, assembly, and test, and in-flight operations. The fact that flight operations are included is part of the end-to-end perspective of this document: with the appropriate investment in S/C architecture, telemetry and fault protection, in flight anomalies could be addressed and corrected. This is felt to be an essential component of a holistic view of supporting long life.

1.3 Effort is Targeted at both Engineering and Science

Many of the practices proposed here derive from the implementation of engineering subsystems, but should apply in most cases to science payloads. Some of those involved in science payloads may not have the background and resources to implement these practices without additional context.

In order that instrument developers could benefit from these guidelines, they would require more insight in how to take advantage of them. As such, this document attempts to provide descriptive information to assist others in not only providing direction, but in identifying tools, resources, and links that could assist them in getting to the finish line.

In developing the guidelines in this document, it is recognized that it is not useful or practical to repeat all of the processes and lessons learned regarding the implementation of space electronics. On the other hand, in an intense radiation environment, some of

these traditional processes require a much higher level of scrutiny and sensitivity. As such, they are included herein, along with content that is unique to this application.

1.4 Introduction to Long Life Guidelines

High radiation environments exacerbate the existing life-degrading mechanisms that interplanetary S/C must contend with. In order to address the radiation effects, efforts are underway to identify rad-hard parts, implement shielding, improve the WCA process, and so on.

In some cases, the degradation from the radiation would overshadow other life-limiting phenomena, so that it is not cost effective to expend much effort in mitigating these other threats. However, there would be many cases where the totality of life-limiting factors need to be taken into consideration in order to extend the lifetime of S/C avionics.

This document attempts to look across the spectrum of life-limiting mechanisms, including radiation, in order to maximize the likelihood of survival. This is of particular importance for a flagship mission that is targeted for a high radiation environment: because the investment in such a mission is so high, we could not afford to allow non-radiation factors to degrade or terminate the mission. By mitigating all the life-limiting mechanisms that we can, we increase the prospects that the flagship S/C would indeed arrive at its destination after perhaps 5 to 10 years in space, prior to exposure to high radiation, and increase the likelihood that it would then complete all its science objectives successfully.

2.0 REFERENCE DOCUMENTS & EXISTING PRACTICE

2.1 JPL D-9899, Long Life/High Reliability Design and Test Rules Study Report

JPL D-9899 was first issued in July 1992; a revised version was published in July 1999. The “Background” section of this document states that:

The planetary programs for the next decade and beyond would include missions with life time requirements in excess of 10 years. Mission concepts requiring 25 and 50-year capability are already being planned. One such mission, Cassini (with a life requirement of 12 years), has been approved and is in the hardware development phase. This study effort was chartered by the Cassini project to determine a set of long life/high reliability design rules which the project should consider implementing. This report represents an independent non-constrained product of the study team and is not intended as a set of requirements on the Cassini project or a representation of the project activities. The Cassini project is using this report as a resource to develop a Project Requirements Document to which compliance could be controlled and deviations identified, assessed, and approved. The Cassini Project Document is the approved source of long life/high

Pre-Decisional: for Planning and Discussion Purposes Only

reliability requirements on the project, and it can be obtained from the project office directly.

2.1.1 Applicability of D-9899

A thorough review of this document was conducted in order to utilize it for this application. Clearly, since the Cassini S/C explored the Saturnian system, it's lifetime guidelines did not address the high radiation exposure of the Jovian system. Furthermore, the structure of this document almost entirely consists of a tabulation of useful processes and practices at the HW level, many of which are part of standard operating practices.

To take an example, Requirement 140 of this document states that with regard to "Burn-In" that "All flight parts shall be burned-in. Burn-ins shall not be performed at stress levels which introduce new failure mechanisms or for durations which would consume excessive life."

Given that these individual guidelines and rules make perfectly good sense, the "divide and conquer" focus at the HW level taken in this document does not address numerous additional perspectives, starting from system design through analysis and test, that could contribute to the overall lifetime of a mission.

As such, while many of the proposed processes in D-9899 remain useful and should be utilized, it was not felt to be appropriate to frame this document as an extension of D-9899. As expounded upon below, the scope of this document is both wider in terms of the perspective that it takes, and yet more focused on the unique challenges of a high radiation environment. The bottom line is that D-9899 should be considered as a useful companion to this document.

In order to capture the results of the review of D-9899, a spreadsheet was generated that includes every one of the 139 individual "Requirements" in the report. For each such requirement, the "OPFM Follow-Up Recommendations" column expresses the relevance of the item to the Outer Planet Flagship Mission. Items that are considered generic good practice were not flagged in this review; the goal was to isolate the items that had some unique and particular relevance to OPFM. This spreadsheet has been included as Appendix A.

2.2 References to Reliability Assurance / Long Life Design Docs

It is not the intent of this document to mirror the multitude of existing guideline documents that deal with reliability assurance and/or long life design guidelines. Many of these documents are quite useful in a generic way, but none of them deals specifically with the challenges of high total dose radiation survival.

Nonetheless, it was deemed useful to at least provide references for a subset of these documents. Links to these documents are provided in Appendix B.

3.0 SYSTEM CONSIDERATIONS & REQUIREMENTS

Even when addressing applications such as a single circuit card, it is useful to approach its implementation as that of a system. While it is useful for organizational purposes to refer to a hierarchy of sub-systems, assemblies, sub-assemblies, and so forth, from a conceptual viewpoint it is logical to consider each level to be a system unto itself. As such, the process of implementing systems applies in a very similar manner to all levels in the traditional hierarchy.

3.1 *Capturing Requirements*

This process needs extra rigor in the OPFM application. Carrying extra capability could have a very high cost for a OPFM, and the rule regarding having a justification for every requirement, supported if possible by a model of operation, is paramount.

3.2 *Flow down Requirements: functional & fault protection*

A very strict adherence to having a complete and accurate representation of flow-down requirements is required. This is particularly the case for adherence to requirements in the Mission Assurance Plan and the Environmental Requirements Document.

3.3 *Self-Imposed requirements*

In order to extend lifetime in a hostile environment, care should be taken to be cautious in levying additional requirements in order to increase performance. By being cautious and conservative in this regard, the HW may be able to sustain significant degradation due to radiation and other factors before it fails functionally.

3.4 *System-Level Verification and Validation (V&V)*

V&V is one of the most critical areas that must be addressed at the system level in order to ensure long life operation. Because of its criticality, a separate section (Section 8.0) in this document entitled “VERIFICATION AND VALIDATION” addresses this subject in detail.

3.4.1 *V&V vs. Development Level*

Each development level must not only ensure that the V&V activities at their level are complete and timely, but should review any related V&V activities at lower and higher levels, to help ensure that the entire fabric of V&V is seamless. This effort should not be left to systems engineers alone, as they may have the knowledge and perspective to see all the gaps.

4.0 ROBUST SYSTEM ARCHITECTURE

4.1 *Inheritance*

Great care should be taken in adopting heritage HW that may not have been intended for extended lifetime operation in a high radiation environment. When heritage HW is chosen, but requires modification of either HW or SW, the effort to do so should not be

underscoped. At times, the time and effort required to adapt HW and SW could turn out to be more costly and less effective than a new design.

4.2 Hardware vs. Software Trade

In extending lifetime, to the first degree it is safer to embed functions in SW rather than HW, since SW does not degrade with time and radiation. However, we must recognize that the more complex behavioral possibilities available in SW could come with a price – must anticipate the overhead required at all levels, up to ATLO, in order to verify and validate the code. SW that does not work could be as lifetime-threatening as HW that does not work.

4.3 Partitioning Functionality into Modules

Carefully architecting a system by decomposing its functions into operational modules could enhance the system lifetime in several ways.

If done correctly, the modules would have well defined interfaces, with a minimum of signals on its inputs and outputs. Such signals should be robust, relatively immune to cross-talk and noise.

A strong modular design would enhance the ability to design, simulate, and test functionality both under normal conditions and under an extensive FP environment.

In dealing with anomalies, both on the ground and in flight, a modular design would simplify the process of trouble-shooting: it would be easier to isolate the problem, simplifying fault trees, and reducing the test and analysis effort required to converge upon the root cause. The net benefit of the above approaches is expected to be an improved likelihood of extended life.

4.4 Model Based Engineering (MBE)

In order to have confidence in the performance and lifetime of avionics HW in an intense radiation environment, MBE becomes a vital part of the development process. Actual testing of all parts and subsystems under expected radiation profile is impossible, and we must rely much more upon analysis and modeling at all levels: part, circuit, assembly, subsystem, and S/C.

4.5 Simulation: Part and Board Level

The use of Computer Aided Engineering (CAE) design and simulation tools is an intrinsic part of MBE, which has the capability to ensure that adequate margins are maintained against all significant aspects of a circuit design: loading, timing, and so on.

When designing for long life, and anticipating a degree of part degradation due to radiation, the margins used for design may be adjusted to ensure that the circuit would operate longer after some degree of component degradation has occurred.

At the part level, such as the design of FPGAs and ASICs, simulation of the circuit timing post-layout would normally provide an excellent predictor of the performance of the manufactured part. The designer of such parts is encouraged to develop a set of test vectors that provide at least 90 % fault coverage, in order to identify sample defects.

At the board level, after the design of the PWB is complete, back-annotation of physical parameters should be used to give a better representation of the behavior of the as-built HW than is available with circuit-only level simulation. Again, greater margins could be maintained in this simulation than is normally the case in order to increase lifetime in the presence of radiation damage to components.

4.6 Power-On vs. Power Off States

In order for MBE to succeed in extending lifetime, a thorough understanding of the relative degradation of S/C avionics under radiation when either powered on or off is essential.

This information may be available based upon the fabrication medium: e.g. CMOS vs. bipolar, FPGA vs. ASIC.

When it is crucial to acquire this information, special tests could be conducted at the component (or even the circuit level).

5.0 FAULT TOLERANCE

5.1 Highly Featured Fault Protection (FP)

In order to have a robust, fault tolerant S/C, a key technique for optimizing the lifetime of OPFM is to have a fully-featured and validated FP system. Typically, S/C FP is designed at a rather high level, such as the assembly or circuit card.

Due to the high radiation level on some of the OPFM, the classes of faults that need to be addressed by FP responses would surely increase, and more complex systems of fault identification and recovery would result, such as fault response trees, tiered FP, and so on.

If possible, for missions subject to a high radiation environment, even failure modes relating to key individual components should be anticipated early in the design cycle, and addressed via the FP system as appropriate.

In general terms, the FP system for a JEO mission should be as comprehensive, well supported, and well-executed, as the state-of-the-art allows. The FP system should allow for inflight adjustments to both the thresholds and the persistence values for identifying faults, should allow selective fault monitors to be turned on and off, and may require a “tiered” fault response, in which the failure of the first response to correct an anomaly leads to an alternate response.

5.2 *Providing Resources for FP*

In order to achieve the benefits of this infrastructure, adequate budget and schedule must be allocated to support this vital activity.

5.3 *Beyond Block Redundancy*

For traditional S/C missions that do not allow Single Point Failures (SPF), block redundancy is typically employed for most S/C engineering subsystems – for critical time dependent functions, such as spacecraft command and control, this block redundancy is enhanced by other mechanisms to ensure that the backup functions are available on a timely basis.

In dealing with strong radiation fields, which could potentially cause damage to both strings in a block redundant configuration, other novel measures could be considered to extend lifetime. For examples, selective additional block redundancy within a single string could be used to protect vital functions whose survival over the mission lifetime is in question.

Techniques such as Triple Modular Redundancy (TMR) with voting logic could be employed to deal with high frequency upset events, such that there is no need for FP intervention.

As good design practice when using TMR, it is advisable to collect telemetry on incidents in which the TMR is actually employed to correct errors.

6.0 PARTS AND MATERIALS

6.1 *Early Part Selection & Generic Parts*

Selection of the most reliable and rad-hard parts and materials is essential for maximizing lifetime. Every effort should be made to procure parts and materials from well-known, qualified sources.

In particular, for high-reliability electronic parts, it is preferable to use suppliers who have a Qualified Manufacturing Level (QML) qualification, which addresses all parts made at a foundry, rather than a more limited Qualified Parts Level (QPL) designation, which addresses a single parts line.

In order to make the above goals achievable, this process should begin very early in the project cycle, such that the required parts could be identified early and tested if necessary. Generic parts that would be needed by multiple S/C subsystems, such as A/D converters, line drivers, voltage references, and so on, should be researched early, even before they are requested for specific applications.

6.2 *Approved Parts and Materials List*

Effort should be made early on to select materials and parts from the APML (Approved Parts and Materials List) that have radiation test data available. Further, those parts where the data is not available, JPL testing budget should be provided for updating and further populating the library. TID/ELDRS (Total Ionizing Dose, High and Low Rate), SEE (Single Event Effects), and DD (Displacement Damage) are some of the radiation effects that should be documented and assessed.

6.3 *Long Lead Time Parts ID & Budgeting*

The advantage of the early identification of parts could be exploited by budgeting resources early to procure them. This also allows bulk buys of common parts, reducing the overall cost of parts acquisition, especially since lot testing could be conducted on a more efficient basis. As a consequence of this approach, risk is also reduced – there would be schedule to recover from defective lots.

6.4 *FPGAs vs. ASICs*

The trade space in choosing between FPGAs and ASICs is very complex and device dependent. In general, because FPGAs are much less tolerant of TID radiation than ASICs, the latter should be preferred for this application. Serious reliability issues have arisen with FPGAs with anti-fuse structures that have largely been eliminated, but there remains the possibility that other anomalies may arise.

6.5 *SEU Mitigation Techniques for FPGAs*

RAM based FPGAs, such as those made by Xilinx, are known to have relatively low thresholds for Single Event Upsets (SEUs). There are various mitigation techniques that could be employed to identify and correct such events, such as the use of Triple Modular Redundant (TMR) flip-flops to maintain state information.

However, since the actual functionality of RAM based FPGAs are contained in their configuration memory, upsets in this area of the FPGA is likely to cause a malfunction. As such, when using such devices, care must be taken to ensure that there are external checks upon the correct functioning of the device, since the anomaly could be corrected by reloading the configuration memory from an external source. The system design must ensure that the time required to identify and correct this fault is acceptable.

6.6 *Special Radiation Tests*

It is expected that for many parts of interest, radiation data is either not available, or incomplete. For example, TID data may have been acquired at a high dose rate in order to complete the testing more efficiently. As such, the annealing effects that could occur at low dose rate testing would not be apparent.

Radiation experts should be consulted to review the part technology, in particular bipolar vs. CMOS, in order to anticipate whether there is “family data” available on a specific part, and to decide if a special parts testing regimen is required.

JPL has an in-house expertise and capability in conducting both high and low dose rate tests, which are typically preceded by a thermal chamber test to ensure the part is within spec. Depending upon the part type, preparation for the test would require test boards and test SW, and an adequate number of parts must be acquired (on the order of 10 to 20).

As a general rule of thumb, the end-to-end cost for radiation testing at JPL, including the NRE, thermal and radiation testing, and a final report, would be approximately \$40K per part.

7.0 MISSION ASSURANCE & QUALITY ASSURANCE

Close coordination with Mission Assurance is of great value in ensuring that no mission assurance requirements violations surface late in the project cycle. This may require that the life-limiting risks be accepted, as there is not enough budget and/or schedule to mitigate them.

Since this close coordination is vital, resources to support this interaction should be anticipated in budgets and work agreements by both the implementing parties, as well as by Mission Assurance. In addition, adequate training needs to be provided to all team members with regard to all the aspects of Mission and Quality assurance processes.

7.1 Problem Reporting System

Extra attention should be devoted to compliance with the Problem Reporting System (PRS): as appropriate, all anomalies should be reported via the PRS, development Problem Failure Reports (PFRs) should be created for Engineering Model (EM) hardware, and all failures and anomalies that occur after flight HW has been powered on should result in PFRs, even when the root cause is understood to be due to facilities and or test equipment.

8.0 VERIFICATION AND VALIDATION (V&V)

8.1 Verification and Validation for a High Radiation Environment

A thorough and extensive V&V regimen is critical in assuring that systems would “do the thing right”, and “do the right thing”. If they fail in these measures, V&V’s usability, and hence the lifetime may be shortened drastically.

As such, V&V requirements and the implementation of the V&V infrastructure must be anticipated from the very earliest stages of conceptual design and architecture, through the Critical Design Review, at which time it should be as mature as the flight HW design.

8.1.1 V&V of Fault Protection System

In order to preserve lifetime in a high radiation environment, in which a wide array of radiation-induced anomalies and failures are expected, Fault Protection (FP) mechanisms, both HW and SW, would be both extensive and detailed. In order to reap the benefits of these mechanisms, adequate resources must be allocated to support the V&V of the fault

protection system – a fault protection mechanism that does not work as planned could not only be life-limiting, but fatal.

The task of V&V for a FP system is challenging for conventional S/C systems, in that the need to simulate and/or stimulate the fault conditions must often be a compromise: for example, one would not actually generate over-currents in flight HW in order to test the FP response. The strategy of using non-standard variants of flight SW to provide a FP trigger is frowned upon, since the test should be performed with a flight SW load rather than a test load. This problem is usually addressed by the use of specialized support equipment (SE) that could mate to flight HW and provide realistic fault triggers.

For a high radiation environment, in which the class of credible faults may be larger than usual, and for which the ability to sustain multiple faults (albeit with limited performance) becomes a goal, the V&V of FP for such a mission is expected to require more budget and schedule than normal. The requirements for specialized SE to support these scenarios must be identified early, to allow for the design and certification of the SE prior to its usage on EM and flight HW.

8.2 Engineering Models (EM): Build Early and in Quantity

Engineering Models could be effective in enhancing operating life. Because they match the flight hardware in fit, form, and function, they provide a very good platform to identify any timing or thermal issues early on that could degrade the margins or operating lifetime of the avionics.

In order to provide these benefits, the development schedule should allow for the build of EMs that would not require extensive modifications to mirror the flight HW. EM FPGAs should be thoroughly tested before the flight FPGAs are programmed. This could ensure that FPGAs do not have to be replaced on the flight boards, perhaps reducing their reliability and perhaps their lifetime.

They should be built early enough so that anomalies identified during EM testing could be corrected on the flight units without compromising their reliability – if need be, a re-spin of the flight boards from EM testing should not be prohibitive.

9.0 ELECTRONIC PACKAGING

The compound effects of shielding due to S/C orientation and structure should be taken into account very early in the design cycle. Transport analysis could assist in determining the actual radiation dosage in a particular S/C location and orientation. For this mission type, it is expected that such analyses would become more the rule rather than the exception.

In this environment, it is recommended that at the Flight System level adequate resources would be provided to support these trades, which are likely to require significantly more resources than previous S/C.

10.0 Packaging Approach

Combined with the best selection process for parts, the system performance of electronic component could be jeopardized by improper packaging materials selection and design. Packaging considerations provide robustness to signal and power transmission, efficient heat dissipation, ESD and EMI shielding, and in general protection from other environmental factors such as chemicals, pollutants & contaminants, and moisture.

Consider utilizing “micro-packaging” (such as Chip-On-Board) in order to reduce volume, and hence shielding mass. The dramatic reductions in both mass and volume that this technology offers (it is being flown on MSL) may be enabling for some instrument providers, and it’s usage in engineering subsystems could free system resources for enhancing the science payload. The ability to free up mass for shielding allows a more conservative exposure of parts to radiation, thus extending the lifetime of the electronics assembly.

10.1 Printed Wiring Board (PWB) Design Approach

The design of printed wiring boards is normally constrained by a set of Design Rule Checks (DRCs) that maintain limits on printed wiring spacing, component placement and so on. In order to increase the likelihood that the PWBs would be manufactured and assembled without defects (especially latent defects that could become apparent after years of usage), it is suggested that the designing to the limits allowed by the DRCs be avoided; for example, the number of layers on the PWB be minimized, even if the result is larger board area and/or quantity of boards.

11.0 THERMAL CONTROL

Careful attention should be paid to providing the correct thermal design for S/C avionics, such as ensuring that the thermal impedance from high power parts to S/C structure is low.

Keeping the junction temperatures of all components well below the 110°C limit is a prudent measure to employ in mitigating the effects of electro-migration and other life-limiting mechanisms. Numerous techniques are available for maintaining parts within appropriate thermal limits, such as mounting drive transistors on special brackets, using wedge-locks and thermal braid, and so on.

11.1 Tighter Control of Flight Operating Temperatures

To the extent that S/C thermal control is able to maintain flight operating temperatures within a favorable and narrow band, lifetime of boards and circuits should be enhanced. The reliability of the PWB and it’s interconnections would benefit from temperature extremes and deep thermal cycles.

For integrated circuits, operating at lower temperatures results in lower equivalent hours of operation; in many cases, this benefit could be determined with confidence with the Arrhenius equation.

In terms of circuit performance, the need to meet requirements over a narrower temperature range makes the design of the circuit easier, increases the likelihood that the circuit could pass its Worst Case Analysis (WCA), and increases the likelihood that it would pass the WCA with significant margin (even though any positive margin would suffice). In turn, having additional margin with regard to WCA could be thought of as contributing to the likelihood that at the end of the nominal mission, the circuit would continue to operate either at full capacity, or with some degree of graceful degradation.

12.0 Transport Analysis: location and orientation of units on S/C

Even if the parts capacity of the parts and boards, taken together with the requisite shielding, complies with the mission requirements, additional shielding could be acquired by taking advantage of the shielding that S/C assemblies provide for each other.

Naturally, the configuration of S/C avionics must take into account numerous factors, such as structural and thermal considerations, distance between units vs. electrical signal integrity, cabling treatment and mass, and so on. As such, it is difficult to take full advantage of such “secondary shielding” early in the project cycle.

Assuming that each S/C box or assembly could meet its shielding requirements on a “stand-alone” basis, the benefit of the secondary shielding provides a larger margin that could compensate for incomplete knowledge of the actual radiation environment and/or the capability of the parts. To the extent that this knowledge is correct, the secondary shielding provides lifetime margin against radiation damage, and improves the likelihood of an extended mission at full capacity.

13.0 RELIABILITY ANALYSIS PROCESS

Typically, flight electronics must undergo a sequence of reliability analyses, including Worst Case Analysis (WCA), Parts Stress Analysis (PSA), and Failure Mode Effects Analysis (FMEA). As part of the effort to reduce the risk of high radiation environments, the standard methods used for Extreme Value Analysis (EVA) approach to WCA at JPL are being reviewed and tailored. It is possible that ultimately PSA and FMEA may be revised as well.

Although the primary thrust of the WCA refinement is to remove excessive conservatism, an effort is being made to “balance the risk” in our WCA approach, which could involve increasing the conservatism in selective areas. The bottom line is to achieve a realistic process that would allow us to utilize the lifetime of parts and materials to their true capability.

13.1 Debugging the Improved Process

Since these refined processes would most likely be exercised for the first time in addressing a hostile radiation environment, it would be of great importance that they be executed early, thoroughly, and with a thorough review process. It would be equally

Pre-Decisional: for Planning and Discussion Purposes Only

important to identify any ambiguities or illogical components of the new process – the new proscriptions should not be followed blindly, since they are in effect being “test driven” by the first users.

14.0 RISK MANAGEMENT SYSTEM

A specific methodology and/or approach for identifying, analyzing and reporting mission risks should be worked out. As a minimum, this Risk Management section should (1) reflect a plan to use the typical ‘risk square’ (mapping risks and consequences across the axes respectively) to characterize task risks consistently, (2) plan for explicit reserves as a risk management approach, and (3) include risk management reporting as an integral part of Risk identification and mitigation strategy.

JPL Project Support organization would provide a guide and workforce support to the project to assure successful risk management in this long-life approach to ground technology development.

The project should impose a comprehensive risk management program to assess and manage risk. The project’s risk management team (e.g., systems engineering, technologists, test engineering, information technology) supported by PIs and the partners would perform continuous risk management throughout the life cycle of the project. The risk management process would conform to the requirements of NPG 7120.5, section 4.3 (e.g., identify, analyze, plan, track, and control). The project would integrate its technology principal investigators’ and partners’ activities into the project’s risk management planning and reporting.

The Project’s approach to risk management would be comprehensive. It would consider not only hardware and software risks, but also peripheral factors (e.g., adequacy of resources and margins, funding cycle, getting on contract, human capital, viability of partnering arrangements, financial condition and capability of partnering organizations, export control issues, proprietary or other sensitive information, safety and health, disaster planning, environment impacts, etc.). The adequacy of risk management approach would be reviewed as part of the internal review process.

Identification of risks and their cost impact would be critical for success of the mission. Risk identification provides quantitative data for risk analysis and the reserve level determination. Great effort would be made during each phase of the mission to have rigorous and thorough process for risk identification and completeness of the risk list to determine adequate reserves for later phase.

Risk identification and assessment would be a continuous project’s responsibility. The project would create a comprehensive Risk List which would involve such information as risk definition, risk maturation date, risk impact stated in dollars, risk probability of occurring, mitigation method and the reserve allocation in dollars. The most modern methods of Project Risk Management would be used to determine appropriate items for the risk list. Such methods include brainstorming, using previous lessons learned, historical data, standard reviews and table-top reviews by objective experts and other

Pre-Decisional: for Planning and Discussion Purposes Only

helpful methods. All types of risks would be included, such as programmatic risks, technical risks, organizational risks and schedule risks.

14.1 Risk Analysis

The Project should utilize quantitative and qualitative tools and metrics in its risk management to evaluate risk probability, uncertainty of estimates, impact/severity, and timeframe. Probabilistic Risk Analysis tools endorsed by JPL flight projects would be applied to the risk list data to establish the appropriate reserve for respective phases of the development.

14.2 Risk Tracking and Control

Risk tracking would be measured primarily against the Project's resource constraints, ability to meet the technical performance commitments and meeting user technology capability needs. The Project's risk management approach would include methods (triggers) to execute and control contingency decisions, to track the effects of the corrective actions, and to accept or close out risks. In addition to the reserve associated with each risk, de-scopes would be applied whenever the reserve impacts exceed the plan.

The risks are placed on the risk matrix below by using the likelihood and consequences of each risk. The red zone indicates that actions must be taken immediately at the start of the project to reduce the likelihood or the consequence of that risk.

Risk Matrix Table

L I K E L Y H O O D	5					
	4					
	3					
	2					
	1					
		1	2	3	4	5

CONSEQUENCE

15.0 EXTENDING LIFE DURING OPERATIONS

In order to extend life during operations, the groundwork for this capability must be established early in the project cycle. Numerous practices could contribute towards achieving this benefit. The groundwork begins at the architecture level, in which a robust, modular architecture is chosen. The use of common elements to support this architecture is also advantageous.

15.1 Need for Higher Observability

Requirements for the elements in this system should stipulate a high degree of observability for key performance parameters. These observables should be accessible to both the S/C as well as ground assets as appropriate, and documented in detail in the flight Commands and Telemetry Dictionary.

15.2 Fully Integrated S/C and Ground Fault Protection

The nominal as well as the anomalous behavior of S/C systems should be characterized in detail based upon the above observables, and integrated into a comprehensive FP system that makes full use of both S/C and ground-based systems. For ground support systems, the capabilities must be in place to have frequent telemetry exchanges with the S/C, and all acquired telemetry data must be analyzed quickly, in order to achieve a rapid response and recovery cycle.

15.3 Complete Parametric Testing of Signatures of Anomalous Behavior

In order to reap the benefits of this infrastructure, the behavior of the integrated S/C must be fully tested under both nominal and anomalous conditions, in order to fully certify the FP system. During this testing, a data base regarding all nominal electrical and thermal states should be generated. Careful attention should be paid to the methods used for stimulating and/or simulating fault conditions; reasonable compromises are often required to provide FP triggers without either risking HW and/or requiring elaborate and expensive ground support equipment.

Appendix A

Main Topics	Subtopics	Review Comments	OPFM Follow-Up Recommendations
Analysis	100 Worst Case Analysis	Only temperature related	Not applicable for radiation
	110 Prelim System And Subsys FMEA By PDR	FMECA is regularly done	
	120 Power Cycling Limited Life Equip	Not related with radiation effects	
Burn-In	130 Flight Part Burn-in	Generic requirement	
	140 Part Burn-in	Generic requirement	
Cables	150 Connector Savers	Generic requirement	
	160 Reusable Devices	Generic requirement	
Components	170 Graceful Degradation	Design such that failures due to exposure beyond expected flight extremes (excessive radiation) will lead to gradual failure	Radiation effects should be studied to avoid catastrophic failure with radiation.
Electrical	180 Silver Migration	Generic requirement	Silver migration due to radiation? Need to find.
	190 Part Stress Derating	WCA data base for SEAWIND: http://rel.jpl.nasa.gov/Projects/SEAWINDS/data/wca-data/1N4148.xls	D-8545 (51-A-04) Deals with JANS1N4148-1 only which is WCA for a diode (Si switching).
	200 EMI Protection	Generic requirement	Does not pertain to radiation effects. Use of Faraday Cage concept for spacecraft isolation (earthing issues may be important). Next item #210 bears on it.
	210 Non-RF Single Path Grounding	Generic requirement	
	220 High Voltage Design	250V and above	
	230 Primary Power Isolation	powerlines to structure isolation of $\leq 10K_{\Omega}$	Not related to radiation.
	240 Engineering Instrumentation	Redundancy of instruments	Depends on availability of resources
	250 Catastrophic Single Event Effects	WCA, FMECA, SEEA	Useful and is in use. Recommend excel analysis sheet developed by Jeffery Nunes for MSL. May require update, e.g. for SEGR.
	260 Part Temp Reduction	Standard practice	Not related to radiation.
	270 Junction Temp Semiconductor	Standard practice	Not related to radiation.

Pre-Decisional: for Planning and Discussion Purposes Only

Main Topics	Subtopics	Review Comments	OPFM Follow-Up Recommendations
	280 Env. Design / test Temp Levels	Standard practice	Revisit thermal excursion ranges combined with radiation effects and possible annealing
Environment	290 Internal ESD Prevention	Maintain internal conductive elements current paths <100M Ω to	May have radiation relevance for high current transients.
	300 Solid Particle Environment	Standard practice	Not applicable for radiation
	310 Environment Compatibility	Standard practice	Not applicable for radiation
	320 External ESD Prevention	Charging environment to be limited to <10V	Related to radiation
	330 Radiation Shielding	Exterior shielding such as to minimize spot shielding.	Consider to follow
	340 Engine Susceptibility To Hypervelocity Impact		Not related to radiation.
	350 Radiation Environment	Use of conservative analyses and/or tests.	Related to radiation.
	360 External Non-conducting Materials	Restricting choice of teflon etc. due to excessive charging	Not directly related to radiation effects on electronics.
	370 Adhesive Joints	fastener backup	Not related to radiation.
Fabrication	380 Electronic Hardware Cleaning	Cleanliness	Not applicable for radiation
	390 Cable Design/fab		Not applicable for radiation
Faults	400 Autonomous Fault Protection / Recovery	Standard practice	Not specifically applicable for radiation
	410 Protection Against Failed RAM	Standard practice	Not specifically applicable for radiation
	420 Fault Trees	For mechanical parts	Not relevant to radiation effects
Handling	430 Shipping, Handling And Storage		Not relevant to radiation effects
Inheritance	440 Inherited Designs	Standard practice	Not applicable for radiation
Materials	450 Non-metallic Materials	N.A.	N.A.
	460 Material Usage	N.A.	N.A.
	470 Metallic Material Selection	N.A.	N.A.
	480 Composite Materials	N.A.	N.A.

Pre-Decisional: for Planning and Discussion Purposes Only

Main Topics	Subtopics	Review Comments	OPFM Follow-Up Recommendations
Mechanical	490 Fluid Filled Device Temp	N.A.	N.A.
	500 Cycling Of Mechanical Devices	N.A.	N.A.
	510 Liquid Lubricated Bearings	N.A.	N.A.
	520 Mechanical Device Complexity	N.A.	N.A.
	530 Force / torque Margin	N.A.	N.A.
	540 Electronic Equipment Venting	N.A.	N.A.
	550 Design For Powered-On Vibration	N.A.	N.A.
Mission Planning	560 Adaptive Mission Strategies	N.A.	N.A.
	570 Propellant Budgets	N.A.	N.A.
Operations	580 Early Device Usage	N.A.	N.A.
	590 Operate Within Test Envelope	N.A.	N.A.
Packaging	600 Design For Rework	N.A.	N.A.
	610 Solder Joint Rework	N.A.	N.A.
	620 Electronic Packaging	N.A.	N.A.
	630 Electronic Packaging Rework	N.A.	N.A.
	640 Conformal Coating Electronic Hardware	N.A.	N.A.
	650 Elec. Package Fatigue Margin	N.A.	N.A.
	660 Elec. Bay Assy. Dynamics Design	N.A.	N.A.
	670 Handling-Induced ESD	N.A.	N.A.
	680 Thermal Shock Design	N.A.	N.A.

Main Topics	Subtopics	Review Comments	OPFM Follow-Up Recommendations
Parts	690 Electronic Part Class	N.A.	N.A.
	700 Limited Life Devices	N.A.	N.A.
	710 Assembly/Installation Of Electronic Parts	N.A.	N.A.
	720 Transformers And Inductors	N.A.	N.A.
	730 Relays	N.A.	N.A.
	740 Transformers-fabrication	N.A.	N.A.
	750 IDDQ Test For CMOS Circuits	N.A.	N.A.
	760 Reed Switches	N.A.	N.A.
	770 Test Structures For Microcircuits	N.A.	N.A.
	780 Capacitors-selection	N.A.	N.A.
	790 Capacitors-derating/leakage	N.A.	N.A.
	800 Capacitors-ceramic	N.A.	N.A.
	810 Capacitors-tantalum	N.A.	N.A.
	820 Selection And Application Of Parts	Look at JPL D-5357	
Power	830 Component Parts And Usage Verification	Standard practice	Not directly related to radiation effects on electronics.
	840 Resistors	Standard practice	Not directly related to radiation effects on electronics.
	850 Critical Item Life Tests	Look for indicators of latent long-life-precluding faults	Not relevant to radiation effects
	860 Power System Design	Standard practice	Not relevant to radiation effects
	870 Power Isolation / protection	Standard practice	Not relevant to radiation effects
Product Assurance	880 Product Assurance Class-A	Per D-1489B for Class A projects	Not directly related to radiation effects on electronics.

Main Topics	Subtopics	Review Comments	OPFM Follow-Up Recommendations
Slip Ring	1080 Slip Ring Run-in	N.A.	N.A.
	1090 Slip Ring Utilization	N.A.	N.A.
	1100 Slip Ring Shorts	N.A.	N.A.
Software	1110 Parameter Range Checking	N.A.	N.A.
	1120 Hardware Control Algorithms	N.A.	N.A.
	1130 Sequence Verification	N.A.	N.A.
	1140 Software Configuration Mgmt / Control	N.A.	N.A.
Structural	1150 Secondary Structure Design	N.A.	N.A.
	1160 Pressure Vessel Design	N.A.	N.A.
Technology	1170 New Technology	N.A.	N.A.
Test Facility	1180 Dedicated Test Hardware	N.A.	N.A.
	1190 System Level HW / SW Integ Testbed	N.A.	N.A.
Testing	1200 Test To Flight Environment	N.A.	N.A.
	1210 Environmental Test Margins	N.A.	N.A.
	1220 Critical Function Tests	N.A.	N.A.
	1230 Failure Free Ops Period	N.A.	N.A.
	1240 Powered Vibration	N.A.	N.A.
	1250 Inherited Designs-solder Thermal Cycle Joint	N.A.	N.A.
	1260 Accel. Life Test	N.A.	N.A.
	1270 Component Databases	N.A.	N.A.

Main Topics	Subtopics	Review Comments	EO Follow-Up Recommendations
	1280 Thermal Shock Test	N.A.	N.A.
	1290 Thermal Cycling/gnd Test	N.A.	N.A.
Thermal	1300 Thermal Cycling	N.A.	N.A.
	1310 Thermal Design Approach	N.A.	N.A.
	1320 Sensitivity To Solar Input	N.A.	N.A.
	1330 Controlled Heat Paths	N.A.	N.A.
	1340 Thermal Design Margin	N.A.	N.A.
	1350 Assembly Operating Temperature	N.A.	N.A.
	1360 Thermal Design In Presence Of A Single Failure	N.A.	N.A.
	1370 Thermal Design Validation	N.A.	N.A.
	1380 System Thermal Design For Fault	N.A.	N.A.
Verification	1390 Design Verification	N.A.	N.A.

Appendix B:

Links to other documents related to system reliability assurance and long life design:

1. Long Life/High Reliability Design and Test Rules Study Report (D-9899), Rev. 2
<http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocID=41972>
2. Safety and Mission Assurance Plan Template, Rev (0)
<http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocID=72652>
3. Reliability Analyses for Flight Hardware in Design (D-5703), Rev. 2
<file:///Users/tdaud/Documents/Work%20%C6%92/MS%20Word%20%C6%92/EJSM%20%C6%92/doc-gw.pl.html>
4. Guidelines for Program/Project Responsibilities for Safety and Mission Success
<http://www.hq.nasa.gov/office/codeq/sms.pdf>
5. Reliability Assurance (D-8671), Rev. 1
<http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocRevID=80732>
6. Electronic Parts Program Requirements for Flight Equipment (D-5357), Rev. 0
<http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocRevID=38712>
7. NASA Spacecraft Design Reference Library:
http://spacecraft.ssl.umd.edu/design_lib/design_lib.html